1991 – 2021
30 YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

Battle of the Sexes: Who Does Cyber-Safety Better ?..Page 1

FREE: Stay Informed With Our Weekly Email Cyber Security Tips ……..Page 2

Security Corner: What is "Ethernet"? ……..Page 3

Top Data Breaches of 2023: Numbers Hit An All Time High……..Page 3

How Small Business Can Approach Technology Modernization ……..Page 4

9 Tips For Setting Up AI Rules For Your Staff……Page 4

February 2024

Kim Nielsen, CISSP, CCSA
President & Chief Technology Strategist at Computer Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

Battle of the Sexes: Who Does Cyber-Safety Better?

Introduction

Are men and women truly significantly different when it comes to cyber-safety?

The answer is both *yes* and *no*! All else being equal, men and women don't display any significant difference in terms of their *vulnerability* to cyberattacks.

There are, however, some key differences in the types of attacks that men and women are more likely to experience.

How does your gender affect your online safety and data privacy? The answer may surprise you.

The Gender Gap in Cyber Attacks

Does this surprise you? Men are more likely to be targeted by phishing attacks, while women are more likely to be targeted by social engineering attacks. Men are also more likely to be victims of malware attacks, while women are more likely to be victims of identity theft.

This isn't because we all have some kind of ingrained weakness to different cybercriminal techniques at birth! Rather, men and women tend to occupy different social roles, and bad actors *do* tailor their threat tactics to specific demographics. For

Continued on pg.2

Continued from pg.1

example, they might send different emails based on what websites you frequent; or depending on the industry you work in. Remember, these trends are general and there are many exceptions. Just because you don't fit the traditional demographic for a scam, doesn't mean they don't happen to anyone!

Think about it like this: Nearly 70% of high-level executives are men. If you were a cyber-thief looking to appeal to CEOs, you might target your language and messages because of that statistic. You might put fake ads on a website for nice suits, or tailor your references accordingly. Meanwhile, because women take over most of the child rearing duties in the average household, someone who wanted to steal from families in a specific neighborhood might develop adware for scam makeup brands or malignant websites purporting to be for kids' toys.

Conclusion

So why *do* different genders experience different threats online? Just like in the real world, it's simply because we have disparate experiences in life. For example, our differences in online behavior, social roles, and economic status. Men are more likely to work in jobs that involve handling sensitive data, which makes them more attractive targets for phishing attacks. Women are more likely to be responsible for household finances, which makes them more vulnerable to social engineering attacks and banking scams.

No matter your gender, it's important to know how to be prepared and protect yourself from ALL kinds of cyber-attacks.

- Be careful about what emails you open and what attachments you download.

- Keep your software up to date, including your operating system, antivirus software, and web browser.

- Use strong passwords and enable two-factor authentication for ALL of your online accounts.

- Be careful about what information you share online.

- Be aware of the latest cyber threats and scams.

By following these tips, *everyone* can reduce their risk of becoming a victim of a cyberattack.

"I DIDN'T KNOW"

Unfortunately, That Excuse Doesn't Replenish Your Bank Account, Resolve A Data Breach Or Erase Any Fines And Lawsuits.

It's coming ...

- That day a hacker steals critical data, rendering your office useless ...
- That day when your bank account or credit card is compromised …
- Or that day when your customers' private lives are uprooted …

Cybercriminals and hackers are constantly inventing NEW ways to infiltrate your company, steal your assets and disrupt your life. The ONLY way to STOP THEM is by CONSTANTLY EDUCATING yourself and your staff on how to PROTECT what's yours!

Now, for a limited time, we have the perfect way to help reduce your risk and keep you safe! Simply sign up to receive our FREE "Cyber Security Tip of the Week." We'll send these byte-sized quick-read tips to your e-mail in-box. Every tip is packed with a unique and up-to-date real-world solution that keeps you one step ahead of the bad guys. And because so few people know about these security secrets, every week you'll learn something new!

Get your FREE "Cyber Security Tip of the Week"
at: https://www.cti-mi.com/224-signup/

Security Corner

What is "Ethernet"?
Do you know what "ethernet" means? Instead of a *wide area network* (WAN) which allows you to connect with others around the world, ethernets are meant to ensure safe and swift communication between devices in close proximity to each other.

What Is Ethernet?
While it's very convenient (and fun!) to hook all of your smart devices up to your home network or buy cool new virtual assistants for your office, connecting smart devices to the local network puts everyone at risk…if you do it with WiFi. Why? The Internet of Things comprises smart software like your Bluetooth doorbell and smart TV, which tend to be more vulnerable to cyberattacks. Once threat actors successfully infiltrate these devices, it's much easier to break into more secure systems on the same network.

Ethernet cables provide a secure and reliable means of data transmission. They allow computers to connect to each other and to the Internet via a local area network (LAN), which connects all devices which are located physically close to one another

What Makes It Safer than the Internet?
Ethernet cables transmit data using encryption protocols, such as AES, which can protect data from being intercepted and read.

Additionally, Ethernet cables can be used to create a physically isolated network—meaning that it's entirely inaccessible from the outside. Added bonus: It also makes your devices run faster since they're hooked into the network directly!

For more information about ethernet, call us at 248-362-3800 or visit: http://tinyurl.com/mt7bnjf6

Top Data Breaches of 2023: Numbers Hit An All Time High

The battle against cyber threats is an ongoing challenge.

Unfortunately, 2023 has proven to be a watershed year for data breaches. Data compromises surged to an all-time high in the U.S.

The last data breach record was set in 2021. That year, 1,862 organizations reported data compromises. Through September of 2023, that number was already over 2,100. In Q3 of 2023, the top data breaches were:

- HCA Healthcare
- Maximus
- The Freecycle Network
- IBM Consulting
- CareSource
- Duolingo
- Tampa General Hospital
- PH Tech

Let's look at the main drivers of this increase in 2023:

1. **The Size of the Surge –** Data breaches in 2023 have reached unprecedented levels. The scale and frequency of these incidents emphasize the evolving sophistication of cyber threats as well as the challenges organizations face in safeguarding their digital assets.

2. **Healthcare Sector Under Siege –** Healthcare organizations are the custodians of highly sensitive patient information. As a result, they've become prime targets for cybercriminals.

3. **Ransomware Reigns Supreme –** Ransomware attacks continue to dominate the cybersecurity landscape. The sophistication of this threat has increased.

4. **Supply Chain Vulnerabilities Exposed** Modern business ecosystems have an interconnected nature. This has made supply chains a focal point for cyberattacks. The compromise of a single entity within the supply chain can have cascading effects.

5. **Emergence of Insider Threats –** The rise of insider threats is adding a layer of complexity to cybersecurity. Organizations must distinguish between legitimate user activities and potential insider threats.

6. **IoT Devices as Entry Points –** The proliferation of Internet of Things (IoT) devices has expanded the attack surface. There's been an uptick in data breaches originating from IoT devices.

7. **Critical Infrastructure in the Crosshairs –** Critical infrastructure has become a prime target of choice for cyber attackers.

8. **The Role of Nation-State Actors –** Nation-state actors are increasingly playing a role in sophisticated cyber campaigns. They use advanced techniques to compromise sensitive data and disrupt operations.

9. **The Need for a Paradigm Shift in Cybersecurity –**The surge in data breaches underscores the need to rethink cybersecurity strategies.

10. **Collaboration and Information Sharing –** Collaboration among organizations and information sharing within the cybersecurity community are critical. Threat intelligence sharing enables a collective defense against common adversaries.

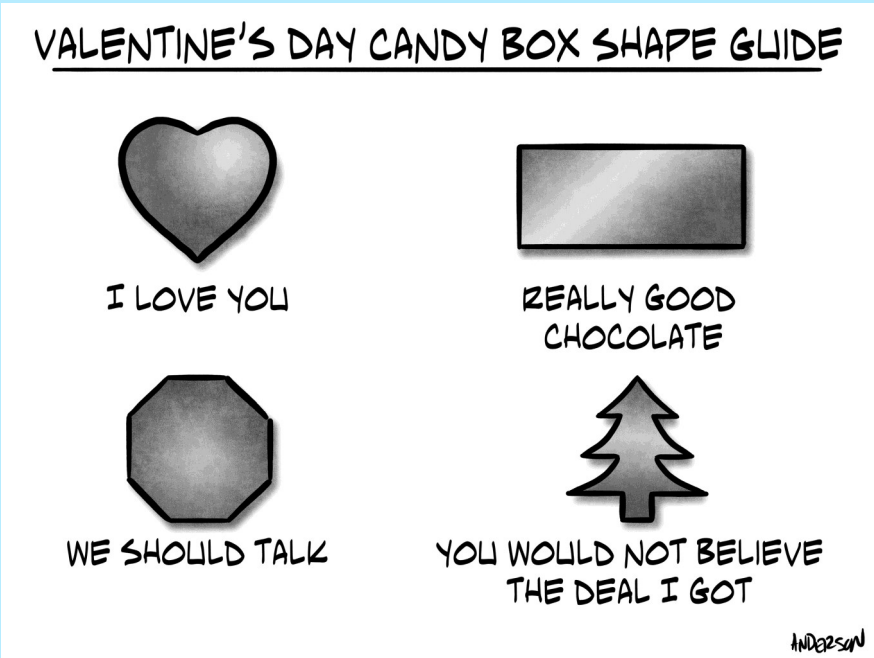
How Small Business Can Approach Technology Modernization

Technology plays a pivotal role in driving efficiency, productivity, and competitiveness. For small businesses, workforce technology modernization is both an opportunity and a challenge.

Embracing modern technology can empower small businesses. It can help them thrive in a digital era. Important benefits include improved employee retention and decreased cybersecurity risk not to mention the productivity and time-saving advantages.

Here are some steps to help your small business get started.

- Assess Your Current Technology Landscape
- Align Technology Goals with Business Objectives
- Focus on Cloud Adoption
- Invest in Collaborative Tools
- Look at Cybersecurity Measures
- Embrace Mobile-Friendly Solutions
- Look at Remote Work Options
- Consider Automation for Efficiency
- Provide Ongoing Training and Support
- Watch and Adapt



9 Tips For Setting Up AI Rules For Your Staff

Artificial intelligence (AI) is a powerful tool. It can enhance the productivity, efficiency, and creativity of your staff.

But AI also comes with some challenges and risks. Businesses need to address and manage these to use AI effectively.

Here are some tips for setting up AI rules for your staff. These tips can help you harness the benefits of AI while avoiding the pitfalls.

1. Define the scope and purpose of AI use.
2. Establish ethical principles and guidelines.
3. Involve stakeholders in the decision-making process.
4. Assign roles and responsibilities.
5. Provide training and support.
6. Ensure data security and privacy.
7. Put a feedback loop in place.
8. Review and update your AI rules regularly.
9. Encourage a growth mindset.